National Infrastructure Protection Center
CyberNotes

Issue #2002-15 *July 29, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 10 and July 25, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Adobe Systems Inc.[1]	Windows	eBook Reader for Windows 2.2	Multiple Denial of Service vulnerabilities exist that could let a malicious user check out all available books regardless of the settings because it doesn't check if you have borrowed the given book already, the loan period is not verified, and when the counter reaches zero the "Add to bookbag" button is still available and working.	No workaround or patch available at time of publishing.	eBook Reader Multiple Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.

[1] Bugtraq, July 19, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
America OnLine[2]	Windows 95/98/ME/ NT 4.0/2000, Mac OS9/X*	Instant Messenger 4.5, 4.7, 4.7.2480	A vulnerability exists due to the way 'aim:' URLs are handled by the client, which could let a malicious user craft arbitrary HTML that will perform unauthorized actions on behalf of the user of a vulnerable client.	The vendor has fixed this issue in versions 4.8 and later.	AOL Instant Messenger Unauthorized Actions	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Andrew Bishop[3]	Multiple	WW - WOFFLE 2.7, 2.7 a, 2.7 b	A buffer overflow vulnerability exists because negative values for the Content-Length component are not handled properly, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.demon.co.uk/pub/unix/httpd/wwwoffle-2.7c.tgz	WWWOFFLE Negative Content-Length Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Apple[4]	MacOS X 10.x	MacOS X 10.0-10.0.4, 10.1-10.1.5	A configuration-related vulnerability exists in MacOS tools because the iDisk authentication credentials are exposed, which could let a malicious user obtain unauthorized access.	Unofficial workaround (Bugtraq): This issue is a problem in the default configuration of Mail.app and may be mitigated by enabling SSL in the client.	MacOS iDisk Default Configuration Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Atrium Software[5]	Multiple	MERCUR Mailserver 3.3, 3.3 SP1&2, 4.0.1, 4.0 1 SP1, 4.2	A buffer overflow vulnerability exists in the Control-Service component due to insufficient bounds checking, which could let a remote malicious user execute arbitrary instructions.	No workaround or patch available at time of publishing.	MERCUR Mailserver Control-Service Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cache Flow[6]	Multiple	CacheOS 3.1.17-3.1.19, 3.1.21, 4.0, 4.0.11-4.0.14, 4.1.06	A Cross-Site Scripting vulnerability exists because user supplied data is not properly sanitized in an unresolved host error page, which could let a malicious user execute arbitrary JavaScript.	This issue is resolved in CacheOS 4.1.07 which is available at: http://download.cacheflow.com/release/CA/4.1.00-docs/CACacheOS41fixes.htm	CacheOS Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
CARE 2002[7]	Unix	CARE 2002 1.0.01 & prior	Multiple vulnerabilities exist: an input validation vulnerability exists in include() statements, which could let a malicious user obtain sensitive information; and multiple SQL injection vulnerabilities exist, which could let a malicious user obtain sensitive information, modify that information, or obtain elevated privileges.	No workaround or patch available at time of publishing.	CARE 2002 Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[2] Bugtraq, July 16, 2002.
[3] Qitest1 Security Advisory #005, July 18, 2002
[4] Bugtraq, July 24, 2002.
[5] Bugtraq, July 17, 2002.
[6] Bugtraq, July 24, 2002.
[7] Securiteam, July 12, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Cascade Soft[8]	Unix	W3Mail 1.0.2-1.0.5	A vulnerability exists due to the way MIME file attachments are stored, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	W3Mail Predictable File Attachment Location	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Caucho Technology[9]	Windows 2000	Resin 2.1.1, 2.1.2	A vulnerability exists when certain DOS devices are requested, which could let a remote malicious user obtain sensitive information.	This issue has been addressed in Resin build 2.1.s020711 available at: http://www.caucho.com/download/index.xtp	Resin Server Device Name Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Cobalt[10]	Unix	Qube 3.0	Several vulnerabilities exist: a vulnerability exists because the authentication mechanism fails to properly validate client cookie input, which could let a remote malicious user bypass the authentication mechanism and obtain administrative privileges; a vulnerability exists if the User account is newly created, which could let a malicious user bypass authentication; and a vulnerability exists because it is possible for a malicious user to delete a file from the server by specifying the path to the file and the first 31 characters of the file.	No workaround or patch available at time of publishing.	Cobalt Qube Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Compaq Computer Corporation[11]	Unix	Tru64 5.0, 5.0 a, 5.1, 5.1 a	A buffer overflow vulnerability exists in the 'su' utility due to insufficient bounds checking, which could let a malicious user execute arbitrary instructions as root.	No workaround or patch available at time of publishing.	Tru64 SU Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Compaq Computer Corporation[12]	Unix	Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	A buffer overflow vulnerability exists in the IPCS utility, which could let a malicious user potentially execute arbitrary code as root.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/	Tru64 IPCS Buffer Overflow CVE Name: CAN-2002-0093	**High**	Bug discussed in newsgroups and websites.
Compaq Computer Corporation[13]	Unix	Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	A Denial of Service vulnerability exists within InetD.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/	Tru64 InetD Denial of Service	Low	Bug discussed in newsgroups and websites.

[8] Nth Dimension Security Advisory, NDSA20020719, July 19, 2002.
[9] KPMG-2002033, July 17, 2002.
[10] SCAN Associates Sdn Bhd Security Advisory, July 23, 2002.
[11] Bugtraq, July 19, 2002.
[12] Compaq Security Bulletin, SSRT0794U, July 16, 2002.
[13] Compaq Security Bulletin, SSRT0795U, July 16, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
David Harris[14]	Windows	Pegasus Mail 4.0 1	A buffer overflow vulnerability exists when long message headers are processed, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Pegasus Mail Message Header Buffer Overflow	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Entercept Security Technologies[15]	Windows NT 4.0/2000, XP, Unix	Entercept Agent 2.5_win32	A vulnerability exists because a local administrator may obtain the password of the 'entercept_agent' account, which could let a malicious administrative user engage in malicious activities on the vulnerable system while concealing their true identity.	Update to versions of Entercept Agent dated after May 21, 2002 available at: http://www.entercept.com/support/	Entercept Agent Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
e-Zone Media Inc.[16]	Multiple	FuseTalk 2.0, 3.0	A Cross-Site Scripting vulnerability exists because user supplied data in not properly sanitized before it is included in the search result page, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	FuseTalk Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Fastlink Software[17]	Multiple	TheServer 1.75	A vulnerability exists because passwords that are contained in the configuration file are stored in plain text, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	TheServer Plain Text Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Geeklog[18]	Unix	Geeklog 1.3.5, 1.3.5 sr1	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists when comments are posted or stories are written because user supplied input is not properly sanitized, which could let a remote malicious user execute arbitrary HTML code; and a vulnerability exists when a malicious user uses the 'Send Email' facility and extra headers are included in the e-mail message, which could let a malicious user obtain sensitive information.	Upgrade available at: http://prdownloads.sourceforge.net/geeklog/geeklog-1.3.5sr2.tar.gz	Geeklog Cross-Site Scripting & Send Email Facility	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[14] SecurityFocus, July 24, 2002.
[15] NTBugtraq, July 10, 2002.
[16] SecurityFocus, July 15, 2002.
[17] SecurityFocus, July 17, 2002.
[18] Bugtraq, July 19, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
GNU[19]	Unix	Mailman 2.0-2.0.11	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists because URI parameters are not properly sanitized, which could let a malicious user execute arbitrary script code; and a Cross-Site Scripting vulnerability exists in the administrative login page because a malicious user may construct a link which will execute arbitrary script code.	Upgrade available at: ftp://ftp.gnu.org/gnu/mailman/mailman-2.0.12.tgz	GNU Mailman Subscribe & Admin Login Cross-Site Scripting Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett Packard Systems[20]	Unix	Instant Support Enterprise Edition	A vulnerability exists which could let an unauthorized malicious user access restricted files.	Patch available at: http://itrc.hp.com Patch PHSS_27411	HP Instant Support Enterprise Edition Unauthorized File Access	Medium	Bug discussed in newsgroups and websites.
Hosting Controller[21]	Windows NT 4.0/2000	Hosting Controller 1.4, 2002	A vulnerability exists because a hidden field is used to specify the username when a password change is performed, which could let a malicious user change the password for that respective user.	Patch available at: http://hostingcontroller.com/English/downloads/inc_updateuser.zip	Hosting Controller Hidden Field Password Changing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[22]	Multiple	Tivoli Management Framework 3.6, 3.6.1, 3.7, 3.7.1	A buffer overflow vulnerability exists in the webserver running on TMR ManagedNodes, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Apply latest Fixpack (Currently Fixpack 2 or Patches 3.7.1-TMF-0066), or apply workaround available at: http://www.tivoli.com/secure/support/documents/security/mgt-fwk-http-vul.html	Tivoli ManagedNode Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
IBM[23]	Unix	Tivoli Management Framework 3.6, 3.6.1, 3.7, 3.7.1	A buffer overflow vulnerability exists in the webserver running on TMR Endpoints when GET commands of excessive length are issued by clients, which could let a remote malicious cause a Denial of Service and possibly execute arbitrary code.	Apply latest Fixpack (Currently Fixpack 2 or Patches 3.7.1-TMF-0066), or apply workaround available at: http://www.tivoli.com/secure/support/documents/security/mgt-fwk-http-vul.html	Tivoli Endpoints Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[19] Bugtraq, July 24, 2002.
[20] Hewlett-Packard Company Security Advisory, HPSBUX0207-0201, July 22, 2002.
[21] Bugtraq, July 13, 2002.
[22] ptl-2002-05, July 15, 2002.
[23] ptl-2002-04, July 15, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
IMHO[24]	Multiple	IMHO Webmail 0.96, 0.96.1-0.96.3, 0.97, 0.97.1, 0.98, 0.98.2, 0.98.3	A vulnerability exists in the Roxen webmail module due to a configuration error, which could let a malicious user gain access to the account of another user.	No workaround or patch available at time of publishing.	IMHO Webmail Account Hijacking	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Macro-media[25]	Windows	Sitespring 1.2 .0	A Cross-Site Scripting vulnerability because the default HTTP 500 error script doesn't check the contents of the error ticket parameter before outputting it, which could let a malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	Sitespring Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Michael Behan[26]	Multiple	CodeBlue 5.1	A buffer overflow vulnerability exists when responses from SMTP servers are processed, which could let a malicious SMTP server execute arbitrary shellcode.	No workaround or patch available at time of publishing.	CodeBlue SMTP Response Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft[27]	Windows NT 4.0/2000	SQL Server 2000 , 2000 SP1&2, SQL Server 2000 Desktop Engine	Several vulnerabilities exist: a buffer overflow vulnerability exists in the Database Consistency Checkers (DBCC) utility because input parameters are not properly sanitized, which could let a malicious user execute arbitrary code; and a SQL injection vulnerability exists in two stored procedures used in database replication, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-038.asp	Microsoft SQL Server 2000 Database Consistency Checkers Buffer Overflow & SQL Server 2000 Replication Stored Procedures Injection CVE Names: CAN-2001-0644, CAN-2002-0645	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[24] SecurityFocus, July 15, 2002.
[25] KPMG-2002032, July 17, 2002.
[26] Bugtraq, July 24, 2002.
[27] Microsoft Security Bulletin, MS02-038, July 24, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
Microsoft[28]	Windows NT 4.0/2000	SQL Server 2000, 2002 SP1&2	Three vulnerabilities exist: two buffer overflow vulnerabilities exist in the resolution service when a maliciously crafted UDP packet is sent, which could let a remote malicious user execute arbitrary code; and a Denial of Service vulnerability exists when a malicious user sends a particular data packet to the SQL server's keep-alive function.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp	Microsoft SQL Server 2000 Multiple Vulnerabilities CVE Names: CAN-2002-0649, CAN-2002-0650	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[29]	Windows 2002	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Profes-sional, 2000 Profes-sional SP1&2, 2000 Server, 2000 Server SP1&2	A vulnerability exists because the username, domain name, and password are read aloud when you log on to a Terminal Services server in a Terminal Services client session.	No workaround or patch available at time of publishing.	Windows 2000 Narrator Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[30]	Windows 95/98/NT 4.0/2000, MacOS 7.0/8.0/ 8.1/ 8.5/ 8.6/9.0, MacOS X 10.0, 10.1	Outlook Express 4.0, 4.27.3110, 4.72.2106, 4.72.3120, 4.72.3612, 5.0, 5.5, 6.0, Outlook Express for MacOS 4.5, 5.0, 5.0.1-5.0.3	A vulnerability exists because it is possible for a client and server to successfully negotiate an encrypted connection without authentication under TLS, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Outlook Express SMTP Over TLS Information Disclosure	Medium	Bug discussed in newsgroups and websites.

[28] Microsoft Security Bulletin, MS02-039, July 24, 2002.
[29] SecurityFocus, July 17, 2002.
[30] Bugtraq, July 19, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
Microsoft[31]	Windows NT 4.0/2000	Exchange Server 5.5, 5.5 SP1&2, IIS 4.0, 5.0	A vulnerability exists in the encapsulated SMTP address, which could let malicious hosts that are not authorized relay e-mail via the SMTP server bypass the anti-relay features and send mail to foreign domains. The vulnerability was originally announced in Microsoft Security Bulletin MS99-027 and reported to affect Exchange Server 5.5. It has been recently reported that this vulnerability also affects the SMTP service included with Microsoft IIS 4.0 and 5.0.	Microsoft announced and released patches for this vulnerability in 1999. At that time it was not reported that the SMTP service for IIS was also affected. There is no patch for the IIS SMTP service. Patch for the Exchange Server is available at: ftp://ftp.microsoft.com/bussys/exchange/exchange-public/fixes/Eng/Exchg5.5/PostSP2/imc-fix/psp2imca.zip	IIS SMTP Service Encapsulated SMTP Address	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.
Microsoft[32]	Windows	Meta-directory Services 2.2	A vulnerability exists in the Microsoft Metadirectory Services (MMS) due to a flaw in the authentication design, which could let a remote unprivileged malicious user obtain administrative access.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-036.asp	Microsoft Metadirectory Services Remote LDAP Client Administration CVE Name: CAN-2002-0697	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[33]	Windows NT 4.0/2000	Exchange Server 5.5, 5.5 SP1-4	A vulnerability exists in the Internet Mail Connector (IMC) component due to an unchecked buffer in the IMC code that generates the response to the EHLO protocol command, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-037.asp	Microsoft Exchange Server IMC EHLO Response Buffer Overflow CVE Name: CAN-2002-0698	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[34]	Windows 95/98/NT 4.0/2000	Outlook Express 5.0, 5.5, 6.0	A vulnerability exists when a certain string of characters is included between the filename and actual file extension, which could let a malicious user malicious user entice a user to open or save files of arbitrary types to their local system.	No workaround or patch available at time of publishing.	Microsoft Outlook Express Spoofable File Extensions	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[31] Portcullis Security Advisory, July 12, 2002.
[32] Microsoft Security Bulletin, MS02-036, July 24, 2002.
[33] Microsoft Security Bulletin, MS02-037, July 24, 2002.
[34] SecurityFocus, July 20, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Mirabilis[35]	Windows 95/98/ME/ NT 4.0/2000, XP	ICQ 2002 a Build 3727, Build 3722	A vulnerability exists because .wav sound files are placed in a predictable location within the installation directory, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Mirabilis ICQ Sound Scheme Remote Configuration Modification & Predictable File Location	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mirabilis[36]	Windows 95/98/ME/ NT 4.0/2000, XP	ICQ, 2001 b Build #3659, #3638, #3636, 2001 a, 2002 a Build #3727, #3722	A remote Denial of Service vulnerability exists when a malicious user sends a large number of graphical emoticons.	No workaround or patch available at time of publishing.	ICQ 2001/2002 Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Mozilla & Netscape[37]	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/9.0.4/ 9.1/ 9.2/ 9.2.1, MacOS X 10.x, Unix	Browser 0.9.2-0.9.9, 1.0, 1.0 RC1&2, 1.0; Netscape 6.0 1, 6.0 Mac, 6.0, 6.1, 6.2-6.2.2	A vulnerability exists because script in the JavaScript protocol is allowed to set and read cookies, which could let remote malicious user obtain sensitive information.	Reportedly, this issue is resolved in the Mozilla Browser 1.1 Beta release.	Mozilla JavaScript URL Host Spoofing Arbitrary Cookie Access	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

Multiple Vendors[38]	Unix	dump 0.4 b10-b29;
		FreeBSD 3.5, 3.5 – STABLE, 3.5.1, 3.5.1 –STABLE/ RELEASE, 4.0, 4.1, 4.1.1, 4.1.1 –STABLE/ RELEASE, 4.2-4.5, 4.2-4.5– STABLE/ RELEASE, 4.6, 4.6 – RELEASE, 5.0;
		NetBSD 1.0-1.5.2;
		OpenBSD 2.0-3.1
			A Denial of Service vulnerability exists when a malicious user creates a file lock on files required for normal operation by the dump utility.	No workaround or patch available at time of publishing.	Multiple Vendor Dump File Locking Denial of Service	Low	Bug discussed in newsgroups and websites.

[35] Bugtraq, July 15, 2002.
[36] Bugtraq, July 24, 2002.
[37] Sandblad advisory #9, July 24, 2002.
[38] asciiSECURE Advisory, July 17, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Multiple Vendors[39]	Unix	FreeBSD 3.5-4.6, 5.0, 3.5 – STABLE, 3.5.1 – STABLE/ RELEASE, 4.1.1 - STABLE/ RELEASE, 4.2 – 4.5 STABLE/ RELEASE, 4.6 – RELEASE; NetBSD 1.0-1.5.2; OpenBSD 2.0-3.1; SuSE. Linux 4.2-8.0	A Denial of Service vulnerability exists when a malicious user creates a file lock on files required for normal operation by the tip utility.	No workaround or patch available at time of publishing.	Tip File Locking Denial of Service	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[40]	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	Microsoft Internet Explorer 5.0, 5.0.1, 5.5, 5.5SP1&2, 6.0; Opera Software Opera Web Browser 6.0.1 win32, Opera Web Browser 6.0.1 Linux, Opera Web Browser 6.0.1	A vulnerability exists because it is possible to define an event handler for the 'onkeydown' event, which could let a malicious user obtain sensitive information	**Microsoft Statement:** "After investigation, our product team has confirmed that this does not meet the bar of a security vulnerability. We will not be releasing a hotfix or patch for this issue." They proposed the following possible workarounds: ? disable or set to prompt - "Submit nonencrypted form data" option ? disable "allow paste operations via script" (best) ? disable active scripting	Multiple Vendor Web Browser JavaScript Modifier Keypress Event Subversion	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[39] asciiSECURE Advisory, July 17, 2002.
[40] Sandblad Advisory #8, July 23, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
Multiple Vendors[41]	Windows 95/98/NT 4.0/2000, MacOS X 10.x, Unix	OpenSSH 2.1-2.3, 2.5-2.5.2, 2.9, 2.9p1&2, 2.9.9, 3.0, 3.0 p1, 3.0.1, 3.0.1p1, 3.0.2, 3.0.2p1, 3.1, 3.1p1, 3.2, 3.2.2p1, 3.2.3 p1, 3.3, 3.3 p1, 3.4, 3.4 p1; SSH Communications Security SSH2 2.0-2.5, 3.0, 3.0.1, SSH2 for Unix 3.1-3.1.2, SSH2 for Win32 3.1-3.1.2	A weakness in the backward compatibility of the SSH Protocol exists due to the fact that a host having the host key for a certain protocol is unlikely to have the host key for the other protocol, which could let a malicious user cause a Man-in-the-Middle attack.	No workaround or patch available at time of publishing.	Multiple SSH Client Protocol Change Default Warning	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Network Associates[42]	Windows 95/98/NT 4.0/2000	PGP 7.0.4, 7.1	A vulnerability exists if the most current patches are applied because cached passphrases doe not expire after the user-specified amount of time and they are stored in memory until a session is terminated, which could let a malicious user compromise the integrity of information encrypted .	Upgrade to 7.1.1	PGP Passphrase Cache Expiration	Medium	Bug discussed in newsgroups and websites.
Novell[43]	Multiple	GroupWise 6.0, 6.0 SP1	A buffer overflow vulnerability exists in the Internet Agent when an overly long string is used as an argument for the 'RCPT TO' field, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	Patch available at: http://support.novell.com/filefinder/12886/beta.html	GroupWise Internet Agent Buffer Overflow	Low/**High** **(High if arbitrary code can b e executed)**	Bug discussed in newsgroups and websites.

[41] Bugtraq, July 23, 2002.
[42] Bugtraq, July 25, 2002.
[43] Bugtraq, July 25, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Novell[44]	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	NetMail 3.0.3, 3.1, XE 3.1,	Several vulnerabilities exist: a buffer overflow vulnerability exists in the 'ModWeb' module, which could let a remote malicious user obtain root privileges; a buffer overflow vulnerability exists in the WebAdmin module, which could let a malicious user execute arbitrary code; and a Denial of Service vulnerability exists in the IMAP Agent when a malicious user sends certain malformed data.	Upgrade available at: http://support.novell.com/servlet/tidfinder/	NetMail Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
NullSoft[45]	Windows 95/98/ME/ NT 4.0/2000, XP	Winamp 2.65, 2.70-2.80	A vulnerability exists because the skin file is placed in a predictable location within the installation directory, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Winamp Skin Predictable File Location	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Oddsock[46]	Windows 95/98/NT 4.0/2000, XP	Song Requester 2.1	Denials of Service vulnerabilities exist in all of the CGI files when a malicious user parses long names or characters to these files.	No workaround or patch available at time of publishing.	Song Requester WinAmp Plugin Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Oracle Corporation[47]	Multiple	Oracle Reports6i 6.0.8, 6.0.8.19. Oracle9iAS Reports 9.0.2	A vulnerability exists in the Reports Server, which could let an unauthenticated remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Oracle Reports Server Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Pablo Software Solutions[48]	Windows 98/NT 4.0, XP	FTP Server 1.0	A Directory Traversal vulnerability exists because the FTP server allows view file content and directory structure of files and directories that reside outside the normally bounding FTP root, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.pablovandermeer.nl/ftp_server.html	FTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[44] PricewaterhouseCoopers Security Vulnerability Report, pwc.20020630, July 15, 2002.
[45] Bugtraq, July 17, 2002.
[46] Outpost24 Advisory, July 16, 2002.
[47] AngryPacket Security Advisory, 0x0004, July 17, 2002.
[48] Securiteam, July 24, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
PHP[49]	Multiple	PHP 4.2.0 4.2.1	A vulnerability exists in the multipart/form-data handler because MIME headers are incorrectly parsed when HTTP POST commands are received, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.php.net/downloads.php	PHP HTTP POST Incorrect MIME Header Parsing	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
PHP[50]	MacOS X 10.0x, Unix	PHP 3.0, 3.0.10 -3.0.18, 3.0.1-3.0.13, 3.0.16, 4.0-4.0.7 RC3, 4.1.0-4.1.2, 4.2.0-4.2.2	A remote Denial of Service vulnerability exists when a malicious user invokes the PHP Interpreter with no command line options.	No workaround or patch available at time of publishing.	PHP Interpreter Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
PHP-Wiki[51]	Multiple	PHP-Wiki 1.2, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3	A Cross-Site Scripting vulnerability exists because HTML is not sufficiently sanitized from URL parameters, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	PHP-Wiki Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Pingtel[52]	Multiple	Expressa 1.2.5, 1.2.7.4	Multiple vulnerabilities exist that affect all aspects of the phone's operation. These vulnerabilities include: remote access to the phone; remote administrative access to the phone; manipulation of SIP signaling; multiple Denials of Service; remote Telnet access (complete control of the VxWorks operating system); and local physical administrative access, which could let a remote malicious user jeopardize critical telephony infrastructure and put an organization's entire network infrastructure at risk.	Pingtel recommends following the "Best Practices for Deploying Pingtel Phones" document available at: http://www.pingtel.com/s_docadmin.jsp They also recommend upgrading to the v2.0.1 software release available at: http://www.pingtel.com/s_upgrades.jsp *Note: This upgrade does not address all of the issues.*	Expressa VoIP phones Multiple Vulnerabilities CVE Names: CAN-2002-0667, CAN-2002-0668, CAN-2002-0669, CAN-2002-0670, CAN-2002-0671, CAN-2002-0672, CAN-2002-0673, CAN-2002-0674, CAN-2002-0675	**High**	Bug discussed in newsgroups and websites. No exploit code is required for some of these vulnerabilities. Vulnerability has appeared in the press and other public media.

[49] e-matters GmbH Security Advisory, July 22, 2002.
[50] Bugtraq, July 23, 2002.
[51] Bugtraq, July 16, 2002.
[52] @stake Inc. Security Advisory, A071202-1, July 12, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Pyramid[53]	Multiple	BenHur Software Update 66	A vulnerability exists due to a weak default firewall configuration ruleset, which could let a malicious user connect and scan internally protected ports.	Update available at: https://www.ben-hur.de/updates_experimental	BenHur Default Firewall Ruleset	Medium	Bug discussed in newsgroups and websites.
Python Software Foundation [54]	Multiple	Python 1.5.2	A vulnerability exists in the Pickle implementation if malicious data is "unpickled," which could let a malicious user execute arbitrary Python commands.	Upgrade available at: http://www.python.org/2.2.1	Python Pickle Unsafe eval() Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Python Software Foundation [55]	Multiple	Python 1.5.2, 1.6, 1.6.1, 2.0, 2.0.1, 2.1, 2.1.1, 2.1.2, 2.1.3	A vulnerability exists in the Pickle implementation if specially crafted malicious object data is "unpickled," which could let a malicious user execute arbitrary Python commands.	Upgrade available at: http://www.python.org/2.2.1	Python Pickle Class Constructor Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Real Networks, Inc.[56]	Windows 95/98/ME/ NT 4.0/2000, XP	RealJuke box 2 for Windows 1.0.2 .379, 1.0.2 .340, RealJuke box 2 Plus for Windows 1.0.2 .379, 1.0.2 .340, RealOne Player Gold for Windows 6.0.10 .505	A buffer overflow vulnerability exists in the parser used for skin files due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Patches available at: http://service.real.com/help/faq/security/bufferoverrun07092002.html	RealJukebox Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Real Networks, Inc.[57]	Windows 95/98/ME/ NT 4.0/2000, XP	RealJuke box 2 for Windows 1.0.2 .379, 1.0.2 .340, RealJuke box 2 Plus for Windows 1.0.2 .379, 1.0.2 .340, RealOne Player Gold for Windows 6.0.10 .505	A vulnerability exists in the 'skin.ini' file due to the way HTML pages are loaded and viewed, which could let a remote malicious user execute arbitrary script.	Patches available at: http://service.real.com/help/faq/security/bufferoverrun07092002.html'	RealJukebox Predictable File Extraction	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[53] Securiteam, July 22, 2002.
[54] Bugtraq, July 17, 2002.
[55] Bugtraq, July 17, 2002.
[56] Shadow Penguin Security Advisory #48, July 12, 2002.
[57] Shadow Penguin Security Advisory #47, July 12, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
Sharman Networks[58]	Windows 95/98/ME/ NT 4.0/2000, XP	KaZaA Media Desktop 1.7.1	A Denial of Service vulnerability exists in the file sharing utility when a malicious user floods the system with a large number of messages.	Update available at: http://www.kazaa.com/en/download.htm	KaZaA Media Desktop Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
SmartMax [59]	Multiple	Software MailMax 4.8	A buffer overflow vulnerability exists in the POP3 daemon, 'popmax,' when an overly large value is submitted for the 'USER' argument, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MailMax Popmax Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Summit Computer Networks[60]	Windows NT 4.0/2000	Lil'HTTP 2.1, 2.2	A Cross-Site Scripting vulnerability exists in the 'pbcgi.cgi' script, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Lil' HTTP 'pbcgi.cgi' Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro-systems, Inc.[61]	Unix	Sun Fire 280R, V480, V880	A Denial of Service vulnerability exists if a malicious unauthorized user alters the environmental monitoring subsystem.	Patch available at: http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=110460&method=f Patch 110460-20	Sun Fire Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[62]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6 _x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the Volume Manager (vold), which could let a malicious user gain unauthorized root access and execute arbitrary code.	Patches available at: http://sunsolve.sun.com Patch 104011-02, Patch 104010-02, Patch 107619-04, Patch 107618-04, Patch 107260-04, Patch 107259-04, Patch 108969-07, Patch 108968-07	Solaris Volume Manager Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[63]	Unix	i-Runbook 2.5.2	A vulnerability exists in the 'none.php' file because it can be manipulated to view files or folders on the server, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	i-Runbook Directory And File Content Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro-systems, Inc.[64]	Unix	Java Web Start 1.0, 1.0.1, 1.0.1_01, 1.0.1_02,	A vulnerability exists because image files that are referenced in the Java Network Launching Protocol (JNLP) file are stored in a predictable location, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Java Web Start JNLP Predictable File Location	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[58] Bugtraq, July 25, 2002.
[59] Security Advisory #4, July 23, 2002.
[60] Securiteam, July 18, 2002.
[61] Sun(sm) Alert Notification, 43908, July 22, 2002.
[62] Sun(sm) Alert Notification, 45707, July 10, 2002.
[63] Portcullis Security Advisory, July 11, 2002.
[64] Bugtraq, July 17, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Sun Microsystems, Inc.[65]	Windows	PC NetLink 1.0, 1.1, 1.2	A vulnerability exists because ACL controls on backup restored files may be reset, which could let a malicious user obtain sensitive information.	Workaround available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F27807	PC NetLink Backup Restoration ACL Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[66]	Windows 95/98/ME/ NT 4.0/2000, XP	Norton Internet Security 2001, Norton Personal Firewall 2001 3.0.4.91	A buffer overflow vulnerability exists in the HTTP proxy due to the inability to handle large requests, which could let a malicious user potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Norton Personal Firewall/ Internet Security 2001 Buffer Overflow CVE Name: CAN-2002-0663	**High**	Bug discussed in newsgroups and websites.
Thorsten Korner[67]	Unix	123tkShop 0.2, 0.3, 0.3.1	A SQL injection vulnerability exists because user supplied data that is used to construct SQL statements and special characters is not properly escaped, which could let a malicious user pass malicious data to the system which modifies SQL queries.	No workaround or patch available at time of publishing.	123tkShop SQL Injection	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Thorsten Korner[68]	Unix	123tkShop 0.2, 0.3	A vulnerability exists if 'register_globals' is enabled, and 'magic_quotes_gcp' is disabled in the PHP configuration file, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://unc.dl.sourceforge.net/sourceforge/my123tkshop/123tkShop-0.3.1.tar.gz	123tkShop Arbitrary File Include	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
TightVNC[69]	Multiple	TightVNC 1.2 .0, 1.2.1	A vulnerability exists because DES challenges are repeated if multiple connections are initiated in rapid sequence, which could let an unauthorized malicious user obtain access.	No workaround or patch available at time of publishing.	TightVNC Repeated Challenge	Medium	Bug discussed in newsgroups and websites.
Trend Micro[70]	Windows NT 4.0	InterScan VirusWall for Windows NT 3.52	A vulnerability exists if a malicious e-mail server adds extraneous whitespace in certain e-mail headers, which could let a remote malicious user create a malicious e-mail that would bypass virus protection.	Patch available at: ftp://ftp-download.trendmicro.com.ph/Gateway/isnt/Hotfix_build1466.zip	InterScan VirusWall Space Gap Scan Bypass CVE Name: CAN-2002-0637	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[65] Sun(sm) Alert Notification, 27807, July 22, 2002.
[66] @stake, Inc. Security Advisory, A071502-1, July 15, 2002.
[67] SecurityFocus, July 16, 2002.
[68] SecurityFocus, July 16, 2002.
[69] Bugtraq, July 24, 2002.
[70] Securiteam, July 17 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Ultrafunk[71]	Windows 95/98/ME/ NT 4.0/2000, XP	Popcorn 1.20	Multiple remote Denial of Service vulnerabilities exist when a malicious user sends a message that contains an unusual amount of data, a malformed string of characters in the subject field, or a when the year in the date field is higher than 2037.	Popcorn is no longer being maintained.	Popcorn Multiple Remote Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Uninet[72]	Windows, Unix	StatsPlus 1.25 Windows, 1.25 Unix	A vulnerability exists because HTML is not properly sanitized before it is written to the 'stat.html' document, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	StatsPlus HTTP Header HTML Injection	**High**	Bug discussed in newsgroups and websites.
University of Washington[73]	Unix	Pine 4.20, 4.21, 4.30, 4.33, 4.44	A Denial of Service vulnerability exists when a malicious user sends a MIME encoded mail with a blank boundary.	Patch available at: ftp://ftp.cac.washington.edu/imap/imap-2002.RC2.tar.Z The contents of this file can be put in place of the "imap" directory in the pine distribution, after which building pine will make use of the new c-client code (consequently, you will need to change SET_DISABLE AUTOMATICSHARED NAMESPACES to SET_DISABLEAUTO SHAREDNS in pine/pine.c).	Pine Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Van Dyke Technologies[74]	Windows 98/98/ME/ NT 4.0/2000, XP	SecureCRT 3.4-3.4.5, 4.0 beta	A buffer overflow vulnerability exists when an overly long SSH1 protocol identifier string is handled, which could let a malicious user execute arbitrary code.	Upgrades available at: http://www.vandyke.com/products/securecrt/security07-25-02.html	SecureCRT Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[71] Securiteam, July 12, 2002.
[72] Bugtraq, July 25, 2002.
[73] Bugtraq, July 24, 2002.
[74] VanDyke Technologies Security Advisory, July 25, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
Visual Shapers[75]	Multiple	ezContents 1.40, 1.41	Multiple vulnerabilities exist: a vulnerability exists in the image file upload function, which could let a malicious user fool the server into treating any file that is readable as an uploaded file; a Directory Traversal vulnerability exists in the Maintain Images function, which could let a malicious user obtain sensitive information; a vulnerability exists in the administrative scripts because they don't check to see if you're currently logged in, which could let a malicious user POST data to several scripts without being logged in; a vulnerability exists because user input is not properly sanitized, which could let a malicious user execute arbitrary script code; and a SQL injection vulnerability exists which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	ezContents Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
VMWare[76]	Windows NT	GSX Server 2.0	A buffer overflow vulnerability exists due to the way arguments are handled to the 'GLOBAL' command, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.vmware.com/download/gsx_security.html	GSX Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
W3C[77]	Windows 2000	Jigsaw 2.2.1	A vulnerability exists when '/aux' is requested twice, which could let a malicious user obtain sensitive information and unauthorized access.	Upgrade available at: http://jigsaw.w3.org/Devel/classes-2.2/20020711/jigsaw.jar	Jigsaw Device Name Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
W3C[78]	Windows 2000	Jigsaw 2.2.1	A Denial of Service vulnerability exists when a malicious user makes certain HTTP requests for DOS device files.	Upgrade available at: http://jigsaw.w3.org/Devel/classes-2.2/20020711/jigsaw.jar	Jigsaw DOS Device Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[75] Bugtraq, July 25, 2002.
[76] Bugtraq, July 24, 2002.
[77] KPMG-2002031, July 17, 2002.
[78] KPMG-2002034, July 17, 2002.

			Vulnerability/ Impact	**Patches/Workarounds/ Alerts**	**Common Name**		**Attacks/ Scripts**
Working Resources Inc.[79]	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	BadBlue Enterprise Edition 1.7.3, BadBlue Personal Edition 1.7.3	Multiple vulnerabilities exist: a vulnerability exists when a malformed version of an HTTP-escaped NULL byte is sent to the server, which could let a remote malicious user obtain sensitive information; a vulnerability exists because passwords contained in the configuration file are stored in plain text, which could let a remote malicious user obtain sensitive information; and a Denial of Service vulnerability exists when a malicious user sends a specially crafted GET request.	No workaround or patch available at time of publishing.	BadBlue Multiple Vulnerabilities	Low/ Medium (Medium if sensitive informa-tion is obtained)	Bug discussed in newsgroups and websites. Exploit has been published for the HTTP-escaped NULL byte vulnerability. There is not exploit required for the password vulnerability.
Working Resources Inc.[80]	Windows 95/98/ME/ NT 4.0/2000, XP	BadBlue Enterprise Edition 1.7, 1.7.2-1.7.4, BadBlue Personal Edition 1.7, 1.7.2-1.7.4	A Cross-Site Scripting vulnerability exists because input is not properly sanitized when a 302 response is returned, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	BadBlue 302 Message Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Working Resources Inc.[81]	Windows 95/98/ME/ NT 4.0/2000, XP	BadBlue Enterprise Edition 1.7, 1.7.2-1.7.4,	A vulnerability exists because administrative interface control access is not sufficiently restricted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BadBlue Administrative Interface Arbitrary File Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Yann Ramin[82]	Unix	ATPhttpd 0.4 b	Several buffer overflow vulnerabilities exist in the source code, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	ATPhttpd Buffer Overflow Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
ZyXEL[83]	Multiple	Prestige 310, 642R	A Denial of Service vulnerability exists when a malicious user sends a malformed TCP packet.	No workaround or patch available at time of publishing.	Prestige Router Malformed TCP Packet Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

[79] Bugtraq, July 13, 2002.
[80] Bugtraq, July 19, 2002.
[81] Bugtraq, July 20, 2002.
[82] Qitest1 Security Advisory #004, July 12, 2002.
[83] Bugtraq, July 24, 2002.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 27 and July 12, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 31 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

July 27, 2002	DSR-Php4.2x.c	Script which exploits the PHP HTTP POST vulnerability.
July 25, 2002	**Kazaa-ex.c**	**Script which exploits the KaZaA Media Desktop Denial of Service vulnerability.**
July 25, 2002	Securecrt-exp.c	Script which exploits the SecureCRT Buffer Overflow vulnerability.
July 25, 2002	Securecrtpoc.c	Script which exploits the SecureCRT Buffer Overflow vulnerability.
July 24, 2002	**Codeblue-exp.c**	**Script which exploits the CodeBlue SMTP Response Buffer Overflow vulnerability.**
July 24, 2002	**Jolt.c**	**Script which exploits the Prestige Router Malformed TCP Packet Denial of Service vulnerability.**
July 24, 2002	**Pegasus.zip**	**Exploit for the Pegasus Mail Message Header Buffer Overflow vulnerability.**
July 24, 2002	Vmwareoverflowtest.c	Script which exploits the GSX Server Buffer Overflow vulnerability.
July 23, 2002	Injectso-0.2.tar.gz	A tool that can be used to inject shared libraries into running processes on Linux and Solaris and also provides routines that can be used by injected libraries to easily modify the behavior of the host process by intercepting library function calls.
July 23, 2002	Linux-390-shellcode-devel.txt	Writing shellcode for Linux/390 mainframes that include a port binding shellcode example.
July 23, 2002	Mimedefang-2.16.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.
July 23, 2002	**Mmaxexp.c**	**Script which exploits the MailMax Popmax Buffer Overflow vulnerability.**
July 23, 2002	Nmap-2.99rc1.tgz	A utility for port scanning large networks.
July 23, 2002	**Php-apache.c**	**Script which exploit the PHP Interpreter Denial of Service vulnerability.**

July 23, 2002	**Phrack59.tar.gz**	**Phrack Magazine Issue 59 Release Candidate 1 includes the following articles: Handling the Interrupt Descriptor Table, Advances in kernel hacking II, Defeating Forensic Analysis on Unix, Advances in format string exploitation, Runtime process infection, Bypassing PaX ASLR protection, Execution path analysis: finding kernel rootkits, Cuts like a knife, SSHarp, Building ptrace injecting shellcodes, Linux/390 shellcode development, Writing Linux kernel keyloggers, Cryptographic random number generators, Playing with windows /dev/(k)mem, Phrack World News, Loopback, and Linenoise.**
July 23, 2002	Spkproxy1.1.tar.gz	A proxy which uses the SPIKE API to help reverse engineer new and unknown network protocols.
July 23, 2002	**Tracerouteexp.tgz**	**Perl script which exploits the TrACESroute Format String vulnerability.**
July 23, 2002	Writing-linux-kernel-keylogger.txt	Writing Linux kernel based key loggers includes a sample key logger that can log user input and passwords.
July 22, 2002	Spkproxy1.1.tar.gz.	An easy to use generic protocol API that helps reverse engineer new and unknown network protocols that features several working examples.
July 21, 2002	**Oe6_issues.eml**	**Exploit for the Microsoft Outlook Express Spoofable File Extensions vulnerability.**
July 19, 2002	**Tru64_su.pl**	**Script which exploits the Tru64 SU Buffer Overflow vulnerability.**
July 19, 2002	**Tru64suexploit.c**	**Script which exploits the Tru64 SU Buffer Overflow vulnerability.**
July 18, 2002	**Mercrexp.c**	**Script which exploits the MERCUR Mailserver Control-Service Buffer Overflow vulnerability.**
July 17, 2002	Viruswall-space-gap.pl	Perl script which exploits the InterScan VirusWall Space Gap Scan Bypass vulnerability.
July 16, 2002	Gre_sniffing.doc	Document that details the approach, methodology and results of a recent experiment using GRE tunnels to sniff all traffic passing through a Cisco router.
July 16, 2002	Spikev2.4.tar.gz	An easy to use generic protocol API that helps reverse engineer new and unknown network protocols that features several working examples.
July 15, 2002	**Blank.scm**	**Exploit for the Mirabilis ICQ Sound Scheme Remote Configuration Modification & Predictable File Location vulnerability.**
July 12, 2002	**Atp-exploit.c**	**Script which exploits the ATPhttpd Buffer Overflow vulnerabilities.**
July 12, 2002	**Popcorn.c**	**Exploit for the Popcorn Multiple Remote Denial of Service vulnerabilities.**
July 12, 2002	**Popcorn.tgz**	**Exploit for the Popcorn Multiple Remote Denial of Service vulnerabilities.**
July 12, 2002	Realjukebox2_exploit.c	Script which exploits the RealJukebox Buffer Overflow vulnerability.

Trends

? **There has been an increase in scanning for the Apache Chunk Encoding Vulnerability and direct reports of exploitation have been received by CERT/CC. For more information see** http://www.cert.org/current/current_activity.html#Apache**.**

? **A warning has been issued by NIPC regarding a potential vulnerability in numerous versions of the open-source Apache Web Server Software. This vulnerability can allow remote access to the**

system and gives an intruder the ability to take control of the system and execute root level commands. NIPC considers this to be a significant threat due to the large installed base of Apache Servers, the potential for remote compromise, and the level of access granted by this vulnerability. For more information, see NIPC Advisory 02-005, located at: http://www.nipc.gov/warnings/advisories/2002/02-005.1.htm

? **BSD/Scalper.worm is an Internet Worm that spreads over Apache web servers on FreeBSD by using the Chunked Encoding exploit.**

? **Numerous exploit scripts exist which exploit the Apache Chunked-Encoding Memory Corruption vulnerability.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

	Common Name			
1	W32.Klez	Worm	Stable	January 2002
2	Elkern	File Infector	Slight Increase	October 2001
3	W32/Sircam	Worm	Stable	July 2001
4	W32.Yaha	Worm	Slight Increase	February 2002
5	W32./Frethem-Fam	Worm	New to List	June 2002
6	W32.Magistr	File, Worm	Slight Decrease	March 2001
7	W32.Badtrans.B	Worm	Slight Decrease	April 2001
8	PE Funlove.4099	File	Slight Increase	November 1999
9	W32/Nimda	File, Worm	Slight Decrease	September 2001
10	JS.Noclose.E	Trojan	Slight Decrease	May 2002

Note: Virus reporting may be weeks behind the first discovery of infection. A total 206 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 387 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

W32.HLLP.Unzi (Win32 Virus): When W32.HLLP.Unzi runs, it infects .exe files that are in the same folder as the virus by prepending itself to them. It also creates in this same folder a file that has the same file name, but with the .eve extension. This virus has a bug that corrupts the host files as it infects them, making the infected files unrepairable.

W32.HLLW.Ultimax (Alias: W32.Ultimax.Worm) (Win32 Worm): This is a worm that copies itself into the startup folder on open shares. When W32.HLLW.Ultimax is first executed, it copies itself as %windir%\Rdvs.exe and then downloads and runs a file that gives access to a pornographic service. It attempts to connect to random IP addresses, and searches shares to find the %windir% folder on remote computers. If the worm finds the %windir% folder, it then uses various language-dependent variations of the %startup% folder to attempt to guess the name of the %startup% folder and copy itself to that location. If it is successful, then when the computer is rebooted, the worm creates the value "fn" in the registry key:

- ? HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

W32/Holar@MM (Win32 Worm): This mass-mailing worm spreads via e-mail, MSN Messenger, and network shares. It arrives as an attachment with a .PIF extension. The filename is chosen by selecting the filename (without the extension) of a file in the My Documents directory on the infected system. The subject of the message is the same as the filename without the extension. The worm exploits the "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability in Microsoft Internet Explorer to automatically execute the virus on vulnerable systems. When the attachment is run, the worm copies itself to the WINDOWS SYSTEM directory and creates a registry run key to load itself at startup:

- ? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\ZaCker

The web server component is also dropped to the System directory as "CmdServ.exe" and an additional registry run key is created for it:

- ? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\MyLife=C:\WINDOWS\SYSTEM\CmdServ.exe

The webserver serves up the file INDEX.HTM in the System directory, which is also created by the worm. This HTM file contains an IFrame that links to the file "C:\WINDOWS\SYSTEM\WarIII.eml," a copy of the worm. The webserver is used by the worm in conjunction with its MSN Messenger component, which sends messages to users on the MSN contacts list with a link to the infected machine. Additional registry keys are created as markers for the worm, for it to know if certain actions have taken place:

- ? HKEY_LOCAL_MACHINE\Software\Microsoft\HolyWar
- ? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HolyWar

W32.Kitro.E.Worm (Win32 Worm): This is a worm that spreads by e-mail and over the KaZaA network. The viral e-mail characteristics will be one of several different Subjects and Attachments. This worm also inserts a Visual Basic script on the computer.

W32/Lavehn-A (Alias: Bloodhound.W32.VBWORM) (Win32 Worm): This is an e-mail worm which copies itself to C:\windows\system\uhneval.exe and creates the following registry entrys:

- ? HKLM\Software\Microsoft\Windows\CurrentVersion\Run\UHN32 = C:\windows\system\uhneval.exe
- ? HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\UHN32 = C:\windows\system\uhneval.exe

The worm will search the hard disk and delete files with the following extensions: .XLS, .DOC, .MDB, .MP3, .RPT, and .DWG. W32/Lavehn-A will e-mail itself to contacts found in the Outlook address book. The e-mails will have the following characteristics:

- ? Subject line: ADMISION 2003
- ? Message body: PROSPECTO DE ADMISION 2003
- ? Attached file: unheval1.exe

W32.WConn@mm (Win32 Worm): This is a mass-mailing worm that e-mails itself to all e-mail addresses in the Microsoft Outlook Address Book. It is written using the Microsoft Visual Basic programming language. This threat may appear in e-mail in this format:

- ? Subject: Free porn site passwords!
- ? Message: Have this file installed in your system. Enter porno sytes and a password will be given 2 you at instant! Always select ok of installer.
- ? Attachments: SetupFP.exe

W97M.Saver.G (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. The virus attempts to delete from infected documents a macro module that is named "Destrib." After infecting a Word Document, the virus will check if the file "CopAnti.dll" exists in the Microsoft Word directory, for example "C:\Program Files\Microsoft Office\Office," and if it does not, then the virus will save a copy of the infected Document as "CopAnti.dll" in the Microsoft Word directory.

WM97/Opey-BC (Word 97 Macro Virus): This virus changes the Microsoft Word application user information to the following:

? UserName = Alcopaul
? UserAddress = #09193612618
? UserInitials = PGA

It also sets the File Properties information for infected files as follows:

? Author = Alcopaul
? Keywords = #09193612618
? Subject = Twice in a row of filing leave of absence.
? Comments = Year 2000 sucks!! Seems like the Y2K bug has infected me. But I assure you, 1st sem of sy 2001-02 will be the beginning of my new life.

On 26 February, the virus may password protect infected documents with the password "Paul Glenerson B. Amurao" and on 25 February, it will attempt to add the line "echo Today is the last day of filing leave of absence." to C:\autoexec.bat. The virus also removes several options from the Tools menu.

WM97/Pri-AE (Word 97 Macro Virus): This virus will attempt to use Microsoft Outlook to send copies of the current document to all entries in the address book. The e-mail will have the following characteristics:

? Subject line: Message From <username>
? Message body: This document is very Important and you've GOT to read this!!!

On 25 December, WM97/Pri-AE inserts a random number of shapes into the currently open document and also edits autoexec.bat, adding code to format the hard drive on the next reboot.

WORM_BUXTE.A (Aliases: Win32/Buxte.Worm, Backdoor.Buxtehude, W32/Buxthude@MM, BUXTE.A) (Win32 Worm): This memory-resident worm e-mails the infected user's password file (.PWL) to an address specified in its code. To propagate, it sends an e-mail with a copy of itself as attachment to all addresses found in the Microsoft Outlook Inbox folder and the Internet Mail and News folder.

Worm/BWG.I (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the use of the Internet Rely Chat (IRC) network. The worm arrives through e-mail in the following format:

? Subject: PoloRalphLauren NEED part-timers!!!!!
? Body: Polo Ralph Lauren Need YOU!
? Attachment: PoloBoy.vbs

If executed, the worm copies itself in the directory under which it is run using the filename "Polo_Ralph_Lauren.BAT." Once the spreading routine is finished, the created files listed below are then deleted. Additionally, the file "system.ini" gets modified. So that it can spread through IRC, the following file is also modified, "script.ini." It will also try to delete various antivirus software applications, including "avp32.exe, antivir.vdf, tc.exe, scan.dat, tbav.dat, fpw32.dll, and various Norton applications"

WORM_FRETHEM.H (Aliases: W32/Frethem.g@MM, I-Worm.Frethem.h, Win32/Frethem.E@mm, W32/Frethem-Fam, Win32/Frethem.E.Worm) (Win32 Worm): This nondestructive, memory-resident worm propagates via e-mail and has been reported in the wild. It arrives as an attachment to an e-mail with no message body and contains the following details:

? Subject: Re: Your password!
? Message Body: <empty>
? Attachments: Your password placed in password.txt, yourpassword.exe, password.txt

On systems with unpatched Internet Explorer 5.01 and 5.5, the executable file attachment automatically executes when this e-mail message is previewed or opened in Microsoft Outlook and Outlook Express.

WORM_FRETHEM.J (Alias: W32.Frethem.J@mm) (Win32 Worm): This worm has been reported in the wild. It is a memory-resident, mass-mailing worm drops files and creates an autorun entry in the registry. It propagates by sending copies of itself as an attachment in e-mail messages with the following details:

- ? Subject: Re: Your password!
- ? Message body: You can access very important information by this password. DO NOT SAVE password to disk. use your mind now press cancel
- ? Attachments: DECRYPT-PASSWORD.EXE, PASSWORD.TXT

On systems with unpatched Internet Explorer 5.01 and 5.5, the executable file attachment, DECRYPT_PASSWORD.EXE, automatically executes when this e-mail message is previewed or opened in Microsoft Outlook or Outlook Express.

WORM_FRETHEM.K (Aliases: W32.Frethem.K@mm, W32/Frethem.k@MM) (Win32 Worm): This worm has been reported in the wild. It is a non-destructive, memory-resident variant of WORM_FRETHEM.D that propagates via e-mail. The worm exploits the "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), to automatically execute the virus on vulnerable systems. The exe file copies itself to the %WinDir% directory and creates the following registry run keys so that it runs each time Windows is loaded:

- ? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Task Bar=C:\Windows\Taskbar.exe
- ? HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Task Bar=C:\Windows\Taskbar.exe

The default SMTP Server, SMTP E-mail Address, and SMTP Display Name are gathered from the Internet Account Manager:

- ? HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\00000001

This information is used by the worm to carry out its propagation routine. The worm also uses Internet Explorer to send requests to various websites.

WORM_FRETHEM.L (Aliases: Frethem.L, I-Worm.Frethem.L, W32/Frethem) (Win32 Worm): This nondestructive, memory-resident worm is a variant of the WORM_FRETHEM family and has been reported in the wild. It propagates using SMTP and arrives as an attachment to an e-mail. It exploits the "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), to automatically execute the virus on vulnerable systems. The exe file copies itself to the %WinDir% directory and creates the following registry run keys so that it runs each time Windows is loaded:

- ? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Task Bar=C:\Windows\Taskbar.exe
- ? HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Task Bar=C:\Windows\Taskbar.exe

The default SMTP Server, SMTP E-mail Address, and SMTP Display Name are gathered from the Internet Account Manager:

- ? HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\00000001

This information is used by the worm to carry out its propagation routine. The worm also uses Internet Explorer to send requests to various websites. The PASSWORD.TXT file the virus sends simply contains the text:

- ? Your password is W8dqwq8q918213

WORM_FRETHEM.M (Aliases: W32/Frethem.m@MM, I-Worm.Frethem.n, W32/Frethem-Fam) (Win32 Worm): This worm has been reported in the wild. It is a non-destructive, memory-resident variant of WORM_FRETHEM.D arrives as an attachment to an e-mail having the following details:

? Subject: Re: Your password!
? Message Body:You can access very important information by this password. DO NOT SAVE password to disk. use your mind. now press cancel
? Attachment: DECRYPT-PASSWORD.EXE, PASSWORD.TXT

On systems with unpatched Internet Explorer (IE), the file attachments automatically execute when the e-mail message where this worm is embedded is previewed or opened in Microsoft Outlook or Outlook Express.

WORM_FRETHEM.N (Aliases: Frethem.N, I-Worm.Frethem.N, W32/Frethem) (Win32 Worm): This nondestructive, memory-resident worm is a variant of the WORM_FRETHEM family and has been reported in the wild. It propagates via e-mail using SMTP (Simple Mail Transfer Protocol) and arrives as an e-mail attachment. On systems with unpatched Internet Explorer (IE), the file attachments automatically execute when the e-mail message where this worm is embedded is previewed or opened in Microsoft Outlook or Outlook Express without the target user clicking or opening said attachments.

WORM_FRETHEM.O (Aliases: W32/Frethem.o@MM, I-Worm.Frethem.o) (Win32 Worm): This worm has been reported in the wild. It is a mass-mailing worm that gathers e-mail addresses from Microsoft Outlook Express mailbox files (.DBX files), the Windows Address Book (.WAB file), .MBX, .EML, and .MDB files to send itself via SMTP. The worm exploits the "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability in Microsoft Internet Explorer to automatically execute the virus on vulnerable systems. The exe file copies itself to the %WinDir% directory and creates the following registry run keys so that it runs each time Windows is loaded:

? HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Task Bar=C:\Windows\Taskbar.exe

The default SMTP Server, SMTP E-mail Address, and SMTP Display Name are gathered from the Internet Account Manager:

? HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\00000001

This information is used by the worm to carry out its propagation routine. The worm also uses Internet Explorer to send requests to various websites. The PASSWORD.TXT file the virus sends simply contains the text:

? Your password is W8dqwq8q918213

WORM_FRETHEM.P (Alias: W32/Frethem.p) (Win32 Worm): This is a variant of the W32/Frethem family and has been reported in the wild. The executable file is PE-Packed and UPX Packed. The worm goes memory resident and will check for its presence in memory if the executable is run again; only one instance of the worm will be in memory at any time. %Windir%\PLP.ini is created by the worm, which contains data that is randomly generated the first time the file is run. The worm attempts to connect the various web-sites. As the worm is not copied to or referenced in any startup locations, once the worm is taken out of memory it will not run again without manual intervention.

WORM_FRETHEM.Q (Win32 Worm): This worm, another member of the WORM_FRETHEM family, sends e-mail messages with itself as an attachment to all addresses found in the Windows Address Book (WAB). The e-mail messages contain random subject lines.

WORM_MANYMIZE.A (Aliases: Win32.Manymize, I-Worm.Manymize, W32.Manymize@mm) (Internet Worm): This worm propagates by mass-mailing. The infected e-mail message comes with different subjects and bodies and usually arrives with the attachments MI2.EXE, MI2.CHM, MI2.HTM, and MI2.WMV. The worm uses two exploits, namely, the IFrame exploit wherein a user gets infected just by previewing the infected e-mail and an Advanced Streaming Format (ASF) exploit wherein a user gets infected through an exploit executed by viewing a .WMV file.

WORM_REDERPS.A (Alias: SPREADER) (Internet Worm): This worm makes multiple copies of itself in the default shared directory of peer-to-peer (P2P) applications such as BearShare, KaZaA Media Desktops, MORPHeus, and eDonkey 2000. These applications are used mainly for finding, downloading, playing and sharing files with other users that use the same. This worm does not modify registry entries. However, it is potentially destructive since it may overwrite certain EXE files, some of which are application files.

WORM_SECET.A (Alias: W32.Secet.Worm) (Win32 Worm): This mass-mailing worm propagates via Microsoft Outlook, sending itself to all recipients in the infected user's Microsoft Outlook address book. It arrives as the e-mail attachment, "SECRET.COM."

WORM_SURNOVA.A (Aliases: SURNOVA.A, Worm.P2P.Surnova) (Win32 Worm): This memory resident worm uses the Microsoft Messenger (MSN) and KaZaA peer-to-peer (P2P) application to propagate itself.

WORM_URICK.A (Aliases: URICK, URICK.A, W32/Urick@MM) (Win32 Worm): This mass-mailing worm sends copies of itself as an e-mail attachment to all the contacts in the infected user's Microsoft Outlook address book. It arrives in an e-mail message with these details:

? Subject: A Windows Trick

? Message Body:This is a cool Windows Trick. Microsoft has not developed a patch for this because they do not want to. Execute the file attached to learn more of this Windows Trick. If it did not work, use a Linux system instead.

? Attachment: %Variable filename%

This worm also disables the Start button on systems running Windows NT, 2000, and XP.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Ducktoy	**N/A**	**Current Issue**
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.Latinus	N/A	CyberNotes-2002-12

Trojan	Version	CyberNotes Issue #
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	N/A	CyberNotes-2002-11
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
Backdoor.Theef	**N/A**	**Current Issue**
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
Banan.Trojan	**N/A**	**Current Issue**
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/Osiris	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08
Fortnight	N/A	CyberNotes-2002-10
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/NoClose	N/A	CyberNotes-2002-11
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
Liquid.Trojan	N/A	CyberNotes-2002-14
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
PWS-AOLFake	**N/A**	**Current Issue**
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11

Trojan	Version	CyberNotes Issue #
RCServ	N/A	CyberNotes-2002-10
SecHole.Trojan	N/A	CyberNotes-2002-01
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Beway	**N/A**	**Current Issue**
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS.Zevach	**N/A**	**Current Issue**
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Click	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Nuker.Winskill	**N/A**	**Current Issue**
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	**N/A**	**Current Issue**
WbeCheck	N/A	CyberNotes-2002-09
Winshell	**N/A**	**Current Issue**

Backdoor.Ducktoy: This Trojan allows unauthorized backdoor access to an infected server from the Ducktoy client. Although ports to be accessed are configurable on the client, the defaults are 29559 and 59211. Servers may be accessed by name or IP address. The Trojan usually creates the value:

? MS HTML <path to Trojan\file name>

under the registry key:

? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

Backdoor.Theef: This is a configurable backdoor Trojan that allows unauthorized access to an infected server by using the Theef client. The client allows a malicious user to select both the IP address and port to be accessed. It allows for full file upload and download, as well as execution on the remote computer. The server portion copies itself to the computer as %windir%\Lib32.exe, so that it runs when you start Windows. It adds the value:

? UpdateComponent %windir%\Lib32.exe

to the registry key:

? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

In addition, the Trojan allows for customized plug-ins. Four plug-in libraries are distributed with the Trojan.

Banan.Trojan: This is an "e-mail bomber" that sends e-mail to a particular e-mail address. The e-mail address is hard-coded within the Trojan. When Banan.Trojan runs, it does the following:

? It copies two files to the folder from which the Trojan is being run, and then executes both files. The files are:

? Temp$01.exe, which is a copy of a legitimate Flash Player. The data that is required for it to play is appended to the file. This file itself is not malicious.

? Temp#01.exe, which is an e-mail bomber that sends an abusive e-mail message to a particular e-mail address.

PWS-AOLFake: This is a Trojan intending to steal AOL screen name and password data from unsuspecting users. Written in Visual Basic 6.0, the Trojan spoofs an AOL login Window, enticing the user to enter screen name and password. When the 'Ok' button is clicked, the Trojan sends an e-mail notification to its author using a public script library:

? from: THASucker

? from e-mail: ILL_PWS@aol.com

? subject: screen name

? body: password

Trojan.Beway: This is a Trojan horse that attempts to stop the processes of many other programs. When Trojan.Beway is executed, it does the following: First, it checks if the file "Vprot32.exe" exists in the %windir% folder. If the file does not exist, the Trojan will create it. It also adds the value "VirusProt32 %windir%\vprot32.exe" to the registry key:

? HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run

This will cause the Trojan to execute each time that you start Windows. Next, the Trojan attempts to register itself as a service process. At this point, it may also attempt to stop the Navapsvc service. Once the Trojan is running as a service, it will continue the malicious actions by stopping the processes for over 100 other programs. Most of these are processes that belong to antivirus other security software. Finally, the Trojan attempts to download and execute a copy of Backdoor.Subseven. To download this file, the Trojan will first try to resolve the IP address to www.microsoft.com. If this attempt is successful, the Trojan will download a copy of Backdoor.Subseven.

VBS.Zevach: This is a Microsoft Visual Basic script Trojan horse that creates more than 300 copies of itself in the root folder of the C drive. It attempts to open two browser windows to display two images from a website. When VBS.Zevach runs, it does the following:

? It runs two .htm files from the http://www.chistesdechavez.com Web site that simply link to .jpg images.

? It adds the value, "Chavez C:\Chavez.vbs" to the registry key:

  ? HKEY_LOCAL_MACHINE\Software\Microsoft\WINDOWS

? It copies itself as:

  ? C:\Windows\System32\Amanda.scr

  ? C:\Windows\System\C.A.M.vbs

W32.Click (Aliases: Nuker.Click.22, Click Trojan): This is a Trojan Horse/DoS attack tool. This tool allows a malicious user to flood a target computer with network packets that can slow down or crash the system. To be enabled, this tool must be configured and executed manually by the user. This tool's main focus is to target Internet Relay Chat (IRC) servers and clients. It can, however, be used on any range of ports that are specified by the user.

W32.Nuker.Winskill (Alias: Nuke-Nukeit): This is a Trojan horse/tool that is used by malicious users to crash systems by taking advantage of a TCP/IP vulnerability. The tool then floods the targeted system with packets in an attempt to crash the system.

W32.Wabbin (Aliases: CARD.A, W32/Wabbin@MM, WORM_WABBIN.A, I-Worm.Wabbin, Win32/Wabbin.A@mm): This is a Trojan horse that sends a Web link to addresses in the Microsoft Outlook Address Book. The subject of the e-mail message contains the recipient's name along with text that suggests that an electronic greeting card has been created for the recipient. The Trojan also sets the Internet Explorer home page to http:/ /www.rankmypix.com.

Winshell (Alias: Backdoor.Winshell): This is a malicious user’s tool that allows an attacker to remotely control a computer where it is installed. An attacker just has to Telnet to the preconfigured port of the remote computer and a menu is shown. This backdoor's file is packed with UPX file compressor, the port it listens to is configurable. It allows the following operations to be performed on an infected computer:

? Install the backdoor so that it will be launched next time Windows starts

? Removes the entries created when installing from the Windows registry

? Reboot a computer

? Open a shell that allows a computer to be controlled remotely

? Download any file from a given URL

When creating a shell, the backdoor executes "cmd.exe" or "command.com" command interpreter, depending on Windows version, and pipes its output to the attacker.